Anticipation, under 35 U.S.C. § 102, requires that each element of the claim in issue be found, either expressly described or under principles of inherency, in a single prior art reference. ***Kalman v. Kimberly-Clark Corp.***, 713 F.2d 760, 218 USPQ 781 (Fed. Cir. 1983).

Claim 7 recites:

> A method of transmitting a data packet received by a repeater from a transmitting network node on a corresponding repeater port, the method comprising:
>
> identifying one of a plurality of repeater ports serving a destination network node based on a destination address in the data packet;
>
> transmitting the data packet on the one repeater port serving the destination network node by concurrently asserting a transmit enable signal on a corresponding media independent interface; and
>
> ***corrupting transmission of the data packet on other*** repeater ***ports by concurrently asserting a transmit error signal and deasserting the transmit enable signal on the media independent interfaces corresponding to the other*** repeater ***ports***.

Claim 16 recites:

> A repeater system comprising:
>
> repeater ports for communication with respective network nodes via respective repeater media independent interfaces; and
>
> a repeater core comprising:
>
> (1) a table for identifying each network node by its corresponding destination address and the corresponding repeater port, and
>
> (2) a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, the ***security circuit corrupting transmission of the data packet on other of the network ports by concurrently asserting a transmit error signal and deasserting a transmit enable signal on the respective media independent interfaces***.

What is being done in Hayakawa and Judd is substantially different from what is being done in the present invention as represented by independent claims 7 and 16, and in fact, has nothing to do with the present invention. More specifically, the present invention addresses a problem of conventional repeaters ***where any network node can eavesdrop on all packets that***

are transmitted on the network, and hence, an unauthorized workstation may eavesdrop on all data packets by obtaining access to a repeater port.

This problem is addressed in the present invention by an arrangement for secure repeater communications to network nodes where (actual) network data is transmitted for repeater ports serving the destination network node of a given data packet, and ***by transmitting corrupted network data*** (data that intentionally is not actual network data) ***for repeater ports that do not serve the destination network node of the given data packet,*** without the unnecessary generation of symbol errors.

Hence, in the present invention, once a repeater core identifies a repeater port as corresponding to the network node having the destination address specified in the data packet, a security circuit transmits the (actual) data packet on the identified repeater port by asserting the transmit enable signal (TX_EN) on a corresponding media independent interface (for the respective network port that have the destination address specified in the data packet) concurrently with transmitting the transmit data on the signal path of a shared bus. In addition, the security circuit transmits ***corrupt data*** (data that intentionally is not actual network data) ***on repeater ports that correspond to network nodes that do not have the destination address specified in the data packet*** and this is done ***by concurrently asserting the transmit error signal (TX_ER) and deasserting the transmit enable signal (TX_EN)*** on the respective media independent interfaces (for the respective network port that do no have the destination address specified in the data packet). Method claim 7 and combination claim 16 each require these specific features.

These features are simply not disclosed or suggested in Hayakawa or Judd. This is quite understandable since, as noted above, what is being done in Hayakawa and Judd is substantially

different from what is being done in the present invention. Both Hayakawa and Judd are concerned with addressing transmission errors, which the present invention is not.

More specifically, in Hayakawa, when a reception node (of a receiving network device) determines that there has been a reception error, the reception node issues a re-transmission request of data to the transmitting node (of the distinct transmitting network device). There is nothing in Hayakawa, let alone at column 13, lines 7-16, that discloses or suggests anything about "corrupting transmission of the data packet on other repeater ports" (which is clearly intentional) by concurrently asserting a transmit error signal and deasserting the transmit enable signal ***on the media independent interfaces*** corresponding to the other repeater ports", as recited in claim 7, or with "a security circuit for transmitting a data packet on an identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, ***the security circuit corrupting transmission of the data packet on other of the network ports*** (which again, is clearly intentional) by concurrently asserting a transmit error signal and deasserting a transmit enable signal ***on the respective media independent interfaces***", as recited in claim 16. Issuing a re-transmission request of data to the transmitting node, as is done in Hayakawa, is a completely different, and unrelated function.

In Judd, an error recovery system/method is disclosed. More specifically, Judd is concerned with ***recovering from errors occurring during transmission of data between*** (distinct network) ***nodes***. There is nothing in Judd, let alone at column 1, lines 49-65, that discloses or suggests anything about "corrupting transmission of the data packet on other repeater ports" (which is clearly intentional) by concurrently asserting a transmit error signal and deasserting the transmit enable signal ***on the media independent interfaces*** corresponding to the other repeater ports", as recited in claim 7, or with "a security circuit for transmitting a data packet on an

identified one of the repeater ports corresponding to the network node having the destination address specified in the data packet, ***the security circuit corrupting transmission of the data packet on other of the network ports*** (which again, is clearly intentional) by concurrently asserting a transmit error signal and deasserting a transmit enable signal ***on the respective media independent interfaces***", as recited in claim 16.

In the operations described in each applied prior art reference, data is being transmitted **between ports of distinct network devices**. The references are not concerned with what is being transmitting from different ports of a ***single*** network device. Neither reference discloses or suggests a (transmission) port corresponding to the network node having the destination address specified in a (received) data packet from which the (received valid) data packet is transmitted to the specified address, and (at least one) ***another port corresponding to a network node that does not have the destination address specified in a (received) data packet from which corrupted data is*** (intentionally) ***transmitted***. Furthermore, in the present invention, there is no way of determining that the corrupted data transmitted by the ports corresponding to a network node that do not have the destination address specified in a (received) data packet **is in fact corrupted data, or data that is in error**. Clearly, this corresponds with the objective of not allowing an unauthorized workstation to eavesdrop on all (real/uncorrupted) data packets by obtaining access to a repeater port. This is not an objective of either Hayakawa or Judd, let alone being disclosed as something to be addressed.

Finally, clearly, a person of ordinary skill in the art would understand that the corrupt data recited in the present invention is being sent from network ports that correspond to the network nodes not having the destination address specified in the data packet. Consequently, whether there is an error in transmitting (Judd) or receiving (Hayakawa) the corrupt data are not

relevant factors of the present claims, as the corrupt data should not be received by any network node, as it is being sent from a network port not having the destination address specified in the data packet and is intentionally corrupt. The data transmitted is intentionally corrupt so that if an unauthorized workstation obtains access to a repeater port, it will not be able to access to actual data packet(s) transmitted from other repeater ports having the destination address specified in the data packet.

In view of the above, it is clear that anticipation is not established as each element/step of each of claims 7 and 16 is/are not found in Hayakawa or Judd. Thus, claims 7-11 and 16-17 are patentable over Hayakawa and Judd as the Examiner has not established a prima facie case of anticipation. Consequently, it is respectfully requested that the rejection of claims 7-11 and 16-17 be withdrawn, and that these claims be allowed.

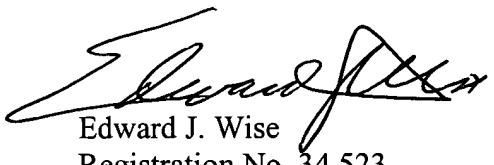
CONCLUSION

Accordingly, it is urged that the application is in condition for allowance, an indication of which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, Examiner is requested to call Applicants' attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Edward J. Wise
Registration No. 34,523

600 13th Street, N.W.
Washington, DC 20005-3096
(202)756-8000 EJW:khb
Facsimile: (202)756-8087
Date: September 26, 2002